

Groupe de travail Réseau
Request for Comments : 3846
 Catégorie : En cours de normalisation
 Traduction Claude Brière de L'Isle

F. Johansson, ipUnplugged
 T. Johansson, Bytemobile

juin 2004

Extension à IPv4 mobile pour porter les identifiants d'accès réseau

Statut du présent mémoire

Le présent document spécifie un protocole Internet en cours de normalisation pour la communauté de l'Internet, et appelle à des discussions et des suggestions pour son amélioration. Prière de se reporter à l'édition actuelle du STD 1 "Normes des protocoles officiels de l'Internet" pour connaître l'état de normalisation et le statut de ce protocole. La distribution du présent mémoire n'est soumise à aucune restriction.

Notice de copyright

Copyright (C) The Internet Society (2004).

Résumé

Lorsque un nœud mobile se déplace entre deux réseaux étrangers, il doit être réauthentié. Si le réseau de rattachement a à la fois plusieurs serveurs d'authentification, d'autorisation et d'identification (AAA, *Authentication Authorization and Accounting*) et des agents de rattachement (HA) en service, le serveur AAA de rattachement peut n'avoir pas d'informations suffisantes pour traiter correctement la réauthentification (c'est-à-dire, pour s'assurer que le même agent de rattachement continue d'être utilisé). Le présent document définit une extension IP mobile qui porte les identités pour les serveurs AAA de rattachement et d'agent de rattachement sous la forme d'identifiants d'accès réseau (NAI, *Network Access Identifier*). L'extension permet à un agent de rattachement de passer son identité (et celle du serveur AAA de rattachement) au nœud mobile, qui peut alors la passer au serveur AAA local lorsque il change son point de rattachement. Cette extension peut aussi être utilisée dans d'autres situations qui exigent la communication d'un NAI entre des nœuds IP mobiles.

Table des Matières

1. Introduction.....	1
2. Terminologie des exigences.....	2
3. Extension de portage de NAI.....	2
3.1 Traitement de l'extension de portage de NAI.....	2
4. Sous type d'identité HA.....	3
5. Sous type d'identité AAAH.....	3
6. Considérations sur la sécurité.....	3
7. Considérations relatives à l'IANA.....	4
8. Remerciements.....	4
9. Références normatives.....	4
10. Adresse des auteurs.....	4
11. Déclaration complète de droits de reproduction.....	4

1. Introduction

Lorsque on construit des réseaux, on aimerait bien être capable d'avoir des redondances. Pour ce faire, on peut placer plusieurs serveurs AAA dans un domaine. Lorsque un nœud mobile s'enregistre via un réseau visité, l'authentification va être traitée par un des serveurs AAA dans le domaine de rattachement. Plus tard, lorsque le nœud mobile se déplace dans un autre domaine visité, il doit à nouveau être authentifié. Cependant, du fait de la redondance offerte par le protocole AAA, il n'est pas garanti que l'authentification sera traitée par le même serveur AAAH que la première fois, d'où il peut résulter que le nouveau AAAH ne sache pas à quel agent de rattachement la session a été allouée. Le présent document définit une extension IP mobile qui peut être utilisée pour distribuer les informations nécessaires pour résoudre cela.

De plus, la seule information qui soit normalement disponible sur l'agent de rattachement dans la demande d'enregistrement est l'adresse IP comme défini dans la [RFC3344]. Malheureusement, cela peut n'être pas suffisant car certaines infrastructures AAA (comme Diameter [RFC3588]) utilisent un acheminement fondé sur le domaine ; une telle infrastructure AAA a besoin de savoir l'identité du FQDN de l'agent de rattachement pour être capable de traiter correctement l'allocation de l'agent de

rattachement. Une recherche inverse de DNS divulguerait seulement l'identité de l'interface IP mobile pour cette adresse IP d'agent de rattachement, qui peut avoir ou non une correspondance univoque avec l'identité FQDN de l'agent de rattachement. C'est la raison pour laquelle l'agent de rattachement doit aussi inclure sa propre identité dans la réponse d'enregistrement. L'extension IPv4 définie dans le présent document a aussi un sous type qui permet de faire ceci. L'identité d'agent de rattachement peut alors être incluse par le nœud mobile dans les demandes d'enregistrement ultérieures lorsque il change de point de rattachement.

2. Terminologie des exigences

Les mots clés "DOIT", "NE DOIT PAS", "EXIGE", "DEVRA", "NE DEVRA PAS", "DEVRAIT", "NE DEVRAIT PAS", "RECOMMANDE", "PEUT", et "FACULTATIF" en majuscules dans ce document sont à interpréter comme décrit dans les BCP 14, [RFC2119].

La terminologie relative à IP mobile décrite dans la [RFC3344] est utilisée dans le présent document. De plus, les termes suivants sont utilisés :

AAAH : un des divers serveurs AAA possibles dans le réseau de rattachement.

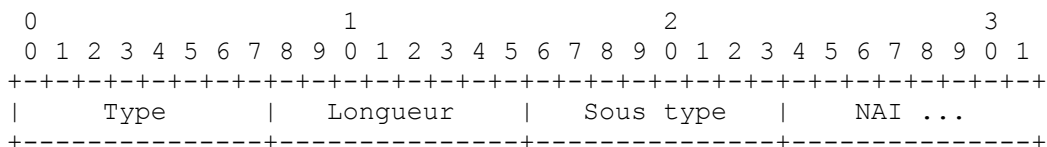
FQDN (*Fully Qualified Domain Name*) : nom de domaine pleinement qualifié.

Identité : l'identité d'un nœud est égale à son FQDN.

NAI (*Network Access Identifier*) : identifiant d'accès réseau [RFC2486].

3. Extension de portage de NAI

Cette section définit l'extension de portage de NAI qui peut être utilisée dans les messages IP mobile de demande et de réponse d'enregistrement, et aussi dans les annonces d'agent IP mobile [RFC3344]. L'extension peut être utilisée par tout nœud qui veut envoyer des informations d'identité sous la forme d'un NAI [RFC2794]. Le présent document définit aussi des numéros de sous type qui identifient le type spécifique de NAI porté dans les sections 4 et 5. Il est prévu que d'autres types de NAI soient définis à l'avenir par d'autres documents.



Type : 136 (sautable) [RFC3344].

Longueur : entier non signé de 8 bits. C'est la longueur de l'extension, en octets, à l'exclusion des champs Type d'extension et Longueur d'extension. Ce champ DOIT être réglé à 1 plus la longueur totale du champ de NAI.

Sous type : ce champ décrit le type particulier de NAI qui est porté dans le champ NAI.

NAI : contient le NAI [RFC2486] dans un format de chaîne.

3.1 Traitement de l'extension de portage de NAI

Lorsque un nœud mobile ou agent de rattachement ajoute l'extension de portage de NAI à un message d'enregistrement, l'extension DOIT apparaître avant toute extension d'authentification.

Dans le cas où l'agent étranger ajoute l'extension de portage de NAI à un message d'enregistrement, l'extension DOIT apparaître avant toute extension d'authentification ajoutée par l'agent étranger.

Si un agent de rattachement a ajouté l'extension de portage de NAI à une réponse d'enregistrement à un réseau mobile, et si il ne reçoit pas l'extension NAI dans les messages de demande d'enregistrement suivants provenant du réseau mobile, l'agent de rattachement peut supposer que le réseau mobile ne comprend pas cette extension de NAI. Dans ce cas, l'agent de rattachement NE DEVRAIT PAS ajouter cette extension NAI aux messages de réponse d'enregistrement à ce réseau mobile.

4. Sous type d'identité HA

L'identité d'agent de rattachement utilise le sous type 1 de l'extension de portage de NAI. Elle contient le NAI de l'agent de rattachement sous la forme `nomd'hôte@domaine`. Ensemble, le nom d'hôte et le domaine forment le FQDN complet (`nomd'hôte.domaine`) de l'agent de rattachement.

Un agent de rattachement qui utilise cette extension DOIT la fournir dans la première réponse d'enregistrement envoyée à un nœud mobile qui n'est pas actuellement enregistré. L'extension a seulement besoin d'être incluse dans les réponses d'enregistrement suivantes si la même extension est incluse dans les demandes d'enregistrement reçues du même nœud mobile.

Un nœud mobile qui utilise cette extension DOIT, si il la reçoit dans un message de réponse d'enregistrement, la fournir dans chaque demande d'enregistrement suivante lorsque la réauthentification est nécessaire. L'échec de la réauthentification, par exemple parce que aucun AAAH n'a pu être joint, va résulter en la terminaison de la session IP mobile. À l'initialisation d'une nouvelle session, un nouvel NAI d'identité d'agent de rattachement peut être fourni au nœud mobile, et les exigences ci-dessus vont s'appliquer au nouveau NAI reçu.

Si le nœud mobile exige un agent de rattachement spécifique et si il a le NAI disponible, il DOIT fournir cette extension dans sa demande d'enregistrement initiale.

Un agent étranger qui reçoit le NAI de l'agent de rattachement par cette extension dans une demande d'enregistrement DEVRAIT inclure le NAI de l'agent de rattachement lorsque il demande l'authentification du nœud mobile à travers l'infrastructure AAA si le protocole AAA utilisé peut porter cette information.

5. Sous type d'identité AAAH

L'identité de AAAH utilise le sous type 2 de l'extension de portage de NAI. Elle contient le NAI du serveur AAA de rattachement sous la forme `nomd'hôte@domaine`. Ensemble, le nom d'hôte et le domaine forment le FQDN complet (`nomd'hôte.domaine`) du serveur AAA de rattachement.

Si il existe plusieurs serveurs AAA dans le réseau de rattachement, un agent de rattachement qui fournit la prise en charge du choix de AAAH conformément au présent document DOIT fournir l'identité de l'AAAH dans la première réponse d'enregistrement qu'il envoie au nœud mobile. L'extension a seulement besoin d'être incluse dans les réponses d'enregistrement suivantes si la même extension est incluse dans les demandes d'enregistrement reçues du même nœud mobile.

Un nœud mobile DEVRAIT sauvegarder la dernière identité d'AAAH reçue dans un message de réponse d'enregistrement et DEVRAIT fournir l'identité d'AAAH dans chaque demande d'enregistrement envoyée lors d'une réauthentification, pour des raisons d'efficacité. L'échec à joindre le AAAH indiqué durant la réauthentification résulterait en le retour d'un nouvel NAI d'identité de AAAH (qui devrait alors être sauvegardé et fourni dans les demandes d'enregistrement suivantes). De même, l'échec de la réauthentification, par exemple parce que aucun AAAH ne peut être joint, va résulter en la terminaison de la session IP mobile ; à l'initialisation d'une nouvelle session, un nouveau NAI d'identité d'AAAH peut être fourni au nœud mobile pour être réutilisé durant des réenregistrements ultérieurs.

Un agent étranger qui reçoit le NAI d'AAAH par cette extension dans une demande d'enregistrement DEVRAIT inclure le NAI d'AAAH fourni lorsque il demande l'authentification du nœud mobile à travers l'infrastructure AAA si le protocole AAA utilisé peut porter cette information.

6. Considérations sur la sécurité

La présente spécification introduit de nouvelles extensions IP mobile qui peuvent être utilisées pour porter les identités de l'agent de mobilité et du serveur AAA, sous la forme d'identifiant d'accès réseau. Les messages IP mobile qui portent cette extension DOIVENT être authentifiés comme décrit dans la [RFC2794], sauf si d'autres méthodes d'authentification ont été acceptées d'un commun accord. Donc, la présente spécification ne diminue pas la sécurité des messages IP mobile.

On notera que les identités envoyées dans les extensions spécifiées ici PEUVENT être envoyées en clair sur le réseau. Cependant, les auteurs n'envisagent pas que cette information puisse créer de problèmes de sécurité.

7. Considérations relatives à l'IANA

Le présent document définit une nouvelle extension IP mobile, et un nouvel espace de numérotation de sous type d'extension IP mobile à gérer par l'IANA.

La Section 3 définit une nouvelle extension IP mobile, l'extension de portage de NAI IP mobile. Le numéro de type pour cette extension est 136. Cette extension introduit un nouvel espace de numérotation de sous type où les valeurs 1 et 2 ont été allouées dans le présent document. L'approbation de nouveaux numéros de sous type d'extension de portage de NAI IP mobile est soumise à révision par experts, et une spécification est exigée [RFC2434].

Le contenu et le format de cette extension n'est pas spécifique des NAI AAA, de sorte que si à l'avenir de nouveaux NAI sont définis qui ne rentrent pas strictement dans la catégorie des NAI AAA, ils pourront néanmoins être traités au sein de l'espace de numérotation de sous type défini pour l'extension de portage de NAI définie dans le présent document.

L'extension de portage de NAI devrait recevoir une valeur de type dans l'espace de numéros de l'IANA pour les extensions IPv4 mobile sautables et dans l'espace de numéros de l'IANA pour les extension d'annonces IPv4 mobile. Idéalement, les numéros alloués de ces deux espaces de numérotation devraient avoir la même valeur.

8. Remerciements

Merci aux auteurs originaux du document GNAIE, Mohamed M Khalil, Emad Qaddoura, Haseeb Akhtar, et Pat R. Calhoun. Le document d'origine a été retiré du mandat du groupe de travail MIP lorsque on n'a pas vu l'utilité de l'extension. Les idées originales ont été réutilisées dans le présent document. Merci aussi à Henrik Levkowitz et Kevin Purser de leurs précieux retours et de leur aide lors de la rédaction du présent document.

9. Références normatives

[RFC2119] S. Bradner, "[Mots clés à utiliser](#) dans les RFC pour indiquer les niveaux d'exigence", BCP 14, mars 1997.

[RFC2486] B. Aboba, M. Beadles, "Identifiant d'accès réseau", janvier 1999. (*Obsolète, voir [RFC4282](#)*) (P.S.)

[RFC2434] T. Narten et H. Alvestrand, "Lignes directrices pour la rédaction d'une section Considérations relatives à l'IANA dans les RFC", BCP 26, octobre, 1998. (*Rendue obsolète par la [RFC5226](#)*)

[RFC2794] P. Calhoun, C. Perkins, "Extension d'[identifiant d'accès à un réseau mobile IP](#) pour IPv4", mars 2000. (P.S.)

[RFC3344] C. Perkins, éd., "Prise en charge de la mobilité IP pour IPv4", août 2002. (*Obsolète, voir [RFC5944](#)*) (P.S.)

[RFC3588] P. Calhoun et autres, "Protocole fondé sur Diameter", septembre 2003. (*Remplacée par la [RFC6733](#)*) (P.S.)

10. Adresse des auteurs

Fredrik Johansson
ipUnplugged AB
Arenavagen 23
Stockholm S-121 28
SWEDEN
téléphone : +46 8 725 5916
mél : fredrik@ipunplugged.com

Tony Johansson
Bytemobile Inc
2029 Stierlin Court
Mountain View, CA 94043
USA
téléphone : +1 650 862 0523
mél : tony.johansson@bytemobile.com

11. Déclaration complète de droits de reproduction

Copyright (C) The Internet Society (2004).

Le présent document est soumis aux droits, licences et restrictions contenus dans le BCP 78, et à www.rfc-editor.org, et sauf

pour ce qui est mentionné ci-après, les auteurs conservent tous leurs droits.

Le présent document et les informations contenues sont fournis sur une base "EN L'ÉTAT" et le contributeur, l'organisation qu'il ou elle représente ou qui le/la finance (s'il en est), la INTERNET SOCIETY et la INTERNET ENGINEERING TASK FORCE déclinent toutes garanties, exprimées ou implicites, y compris mais non limitées à toute garantie que l'utilisation des informations ci-encloses ne violent aucun droit ou aucune garantie implicite de commercialisation ou d'aptitude à un objet particulier.

Propriété intellectuelle

L'IETF ne prend pas position sur la validité et la portée de tout droit de propriété intellectuelle ou autres droits qui pourraient être revendiqués au titre de la mise en œuvre ou l'utilisation de la technologie décrite dans le présent document ou sur la mesure dans laquelle toute licence sur de tels droits pourrait être ou n'être pas disponible ; pas plus qu'elle ne prétend avoir accompli aucun effort pour identifier de tels droits. Les informations sur les procédures de l'ISOC au sujet des droits dans les documents de l'ISOC figurent dans les BCP 78 et BCP 79.

Des copies des dépôts d'IPR faites au secrétariat de l'IETF et toutes assurances de disponibilité de licences, ou le résultat de tentatives faites pour obtenir une licence ou permission générale d'utilisation de tels droits de propriété par ceux qui mettent en œuvre ou utilisent la présente spécification peuvent être obtenues sur le répertoire en ligne des IPR de l'IETF à <http://www.ietf.org/ipr> .

L'IETF invite toute partie intéressée à porter son attention sur tous copyrights, licences ou applications de licence, ou autres droits de propriété qui pourraient couvrir les technologies qui peuvent être nécessaires pour mettre en œuvre la présente norme. Prière d'adresser les informations à l'IETF à ietf- ipr@ietf.org .

Remerciement

Le financement de la fonction d'édition des RFC est actuellement fourni par l'Internet Society.